IS SERVICING – RECEIVER WORKPROGRAM

CHAPTER 22WP

(FILE NAME ON DISK # 3 = IS-WP#18.WPD) ***COMMENTS***

This section is intended to identify services received from financial institutions and/or other businesses and evaluate the adequacy of controls over these services. If information processing services are not received from other corporate entities (including affiliate organizations), completion of this section is not required. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook.*

Tier I

EXAMINATION PLANNING

1. Review the following documents:

   a. The examination scope memorandum issued by the examiner-in-charge (EIC).

   b. Previous examination reports and working papers.

   c. Internal/external audits.

   d. Internal reports and any computer services policies and practices, including corporate contingency plans, information security practices, and end-user/microcomputer policies.

2. Determine any material changes affecting the institution's information processing function since the previous examination by reviewing pertinent internal files and correspondence.

3. Based on the performance of the previous steps and discussions with the EIC, determine the scope and set the objectives for this workprogram section. Select the worksteps necessary to meet examination objectives. Appropriate worksteps can include the following procedures, along with procedures discussed in the workprograms addressing:

   a. Corporate Contingency Planning.

   b. MIS Review.

c. Networking.

d. End-User Computing

e. Retail EFT.

f. ACH

GENERAL

4. If the institution receives major data processing support from one or more outside servicers.

   a. List the name(s) and location(s), of the servicer(s).

   b List any known affiliations between these servicers and either banks or data processing vendors.

   c. Prepare a listing of the services outside vendors provide the institution.

5. Determine if the institution is subject to notification requirements outlined in the Bank Service Corporation Act (See Chapter 24, Laws and Regulations for additional information on this act).

CONTRACTS

6. Review a copy of the contract(s) used and determine if they are in conformance with the guidelines contained in the narrative section of Chapter 22: IS Servicing - Providers and Receivers.

SERVICE QUALITY

7. Determine whether management obtains and reviews information detailing service quality factors. Sources of information could include:

   a. Reports detailing measurable performance indicators. (Eg., up-time, processing results vs. contract performance goals, etc.)

   b. Internal reports evaluating the provider's customer service department.

   c. Institution personnel participation in servicer sponsored or independent user groups addressing common client issues.

d. Employee feedback regarding training provided by the servicer.

FINANCIAL

8. Assess the adequacy of the institution's system for monitoring the financial condition of its servicer(s) and whether the system is sufficient to project the continued viability of contracted services.

   Review and assess the adequacy of any alternate processing plans management has for replacing servicers who reveal signs of financial weakness.

9. Does the institution pay IS related fees to affiliates, shareholders, or insider related companies?

   If so, does management review or audit these transactions?

   Are these transactions in compliance with applicable laws and regulations?

POLICIES AND PROCEDURES

10. Has the board of directors developed and implemented corporate policies or procedures which govern institutional information processing activities, including?

    a. Corporate contingency planning.

    b. End-user computing activities.

    c. Information security.

11. Has management evaluated the adequacy of contingency plans of its servicer(s)?

12. Has management ensured that the institution's contingency plan is compatible with and complements the servicer's?

13. Does management test the adequacy of its corporate contingency plans on an annual basis or in accordance with its plan?

14. Has the directorate reviewed and approved the corporate contingency plan within the last 12 months?

15. Do board minutes adequately reflect directorate approval?

16. Determine how management or the board of directors complies with regulatory policies involving EFT switches and network services. This may include review of outside servicers, including nonfinancial companies, who provide EFT services. It also could include controls over ACH, POS, ATM, or automated bill payment systems.

CONCLUSIONS

17. Review the results of work performed in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

18. Discuss with management:

    a. Violations of law, rulings, regulations or significant internal control deficiencies.

    b. Recommended corrective action for deficiencies cited.

    c. Management's proposed actions for correcting deficiencies.

19. Assign rating. (See Chapter 25 for additional information on FFIEC SP-2: Uniform Interagency Rating System for Data Processing Operations.)

20. Prepare an index of workpapers for this section of the workprogram.

	Comments
21. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include, important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations. (See Chapter 2 for additional information on supervision by risk and supervisory strategies.)	
22. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.	

Examiner | Date

_____|_____

Reviewer's Initials

Tier II

CONTRACTS

1. Do contract provisions specify:

   a. Specific work to be performed by the servicer?

   b. The basis of costs, including development, conversion and processing, and additional charges for special requests?

   c. The established time schedules for receipt and delivery of work?

   d. Responsibilities for security of the communications network?

   e. Audit responsibility, including the right of user representatives to perform audit procedures?

   f. Backup and record protection provisions (equipment, programs, data files) to ensure timely processing by the service center in emergencies?

   g. Servicer disaster recovery plans are provided to the serviced institution for review?

   h. Provisions for sharing disaster recovery plan test results with serviced financial institutions?

   I. Liability for source documents while in transit to and from the service center? (If the service center is responsible, the servicer should have adequate insurance coverage for such liabilities.)

   j. Maintenance of adequate insurance in case of data losses through error and omissions?

   k. Confidential treatment of records?

   l. Ownership of computer programs and related documentation?

   m. Ownership of master and transaction data files and their return in machine readable format upon the termination of the contract or agreement?

n. Price changes, cost and method of canceling the contract, including adequate time allowance?

o. Processing priorities?

p. Notification from the service center to the users of all changes that would affect procedures, reports, etc.?

q. That financial information is to be periodically (preferably annually) provided by the servicer to serviced institutions?

r. Training provisions, including cost, for financial institution personnel?

s. Allowable actions in the event of receivership or bankruptcy?

t. Penalty clauses, if any, for early cancellation of the contract?

u. Prohibitions against assignment of the contract servicing by either party without the prior written consent of the other?

2. Are the terms of the contract appropriate?

3. Did the initiation/continuation of the contract provide any inducements?

   a. If yes, were the inducements properly documented?

   b. Were the inducements appropriate?

FINANCIAL

4. Does the institution's policies, practices, or procedures for monitoring the annual financial performance of its major data processing servicer(s) include:

   a. Reviewing financial information.?

b. Reviewing reports of independent auditors?

c. Reviewing regulatory reports?

d. Reviewing public media (trade papers, TV, etc.)?

e. Presenting the results of these reviews to the board of directors?

AUDIT

5. Does the internal/external audit coverage of the data processing function reflect:

   a. The absence of conflicting duties (independence)?

   b. Sufficient training and experience of auditors (competency)?

   c. An adequate scope?

OPERATIONS

6. Do policies or practices adequately segregate personnel duties and responsibilities in the areas of:

   a. Input preparation and balancing?

   b. Data entry?

   c. Reject reentry?

   d. Balancing of output?

   e. Handling of unposed items?

7. Do procedures or practices for master file change requests (address changes, due dates, interest rates, etc.) address the following:

   a. Require documentation sufficient to document the substance of the transaction?

   b. Identify the originating personnel?

   c. Reconciling of the change report by an independent individual?

8. Are management or the board of directors regularly reviewing exception reports?

9. Does the institution microfilm or otherwise record source documents before the documents are transported to the data center?

10. Are computer-processed negotiable instruments (e.g., blank checks, stock certificates, plastic bank cards) and facsimile signature plates:

    a. Under dual control?

    b. Kept in a locked, secure location?

    c. Issued only as required?

    d. Prenumbered and in sequential order?

    e. Governed by logs that provide for an acceptable audit trail?

    f. Reconciled after each use?

    g. Periodically inventoried?

11. Are listings of unposed entries used to control resubmissions?

12. Are rejected items and lists of captured items independently balanced?

13. Is the operation of equipment limited to personnel who do not perform conflicting duties?

14. Has the institution adequately trained a sufficient number of employees to operate the equipment and thus reduced its dependence on key personnel?

15. Are output reports balanced to general ledger control on a daily basis?

INFORMATION SYSTEMS SECURITY

16. Identify persons with the authority to administer the organization's information systems, and:

a Determine if the number of personnel with security administration authority appears reasonable, given the size and complexity of the institution. Management should limit the number of those persons with security administration authority to only those who are necessary to provide primary and secondary security coverage.

b. Ensure that management limits security administration responsibilities to only those individuals who do not have other conflicting duties.

17. Has senior management provided its primary security administrator with an approved listing of those individuals authorized to grant personnel access to the system?

18. Do security administrators maintain written access authorizations for all users?

    a. Obtain a listing of existing users from the security administrator.

    b. Compare written access authorizations to the listing of resident users.

19. Obtain a listing of all available security exception reports. Determine which exception reports management is utilizing and the individuals responsible for their review.

20. Ensure that the institution's exception report review process appropriately supports relevant separation of duty issues.

	Comments

INSURANCE

23. Obtain a listing of all information system-related insurance coverages. Determine if contracted coverages are sufficient to comply with the guidelines set forth in Chapter 9, Management.

24. Proceed to procedure 17, Tier I.

Examiner | Date

_____|_____

Reviewer's Initials